Préambule

Les mesures exposées ci-dessous visent à satisfaire aux exigences de la réglementation européenne, en particulier le RGPD[1] et l'AI Act[1]. Elles demeurent applicables après la fin du contrat, conformément aux articles 17 et 18 de nos CGV (Conditions Générales de Vente).

⚠ Le présent document n'a, à lui seul, aucune valeur juridique. En revanche, chaque affirmation y est précisément sourcée et renvoie à des documents signés lors de chaque prestation, qui rendent contractuellement opposables l'ensemble des engagements décrits ici (CGV, contrats de prestation, DPA, etc.). Nous pouvons vous transmettre ces documents sur simple demande à rgpd@codesia.fr, dans les meilleurs délais. En cas d'écart entre le présent document et les documents contractuels (CGV/CGP, contrat de prestation, DPA), ces derniers prévalent.

POUR MIEUX COMPRENDRE

1 Le RGPD (2016) et l'AI Act (2024) sont deux règlements européens qui encadrent notre activité chez Codesia. Le RGPD encadre essentiellement la protection et la sécurité de vos données personnelles, tandis que l'AI Act encadre l'usage des systèmes d'intelligence artificielle.

01 Notre environnement de travail

1 Notre serveur est hébergé au sein de l'Espace économique européen

Nous exploitons un serveur privé virtuel (VPS[2]) hébergé dans un centre de données situé au sein de l'Espace économique européen (EEE).

Vos données opérationnelles sont conservées dans cette base, sur nos serveurs, et non chez un fournisseur cloud tiers. Nous y hébergeons et administrons nous-mêmes, notamment :

- **n8n**, l'orchestrateur de nos automatisations
- **PostgreSQL**, notre base de données

Aucune donnée n'est transmise aux éditeurs de ces logiciels.

Le recours à un fournisseur VPS établi renforce la fiabilité et la continuité de service par rapport à une solution auto-hébergée, en réduisant les interruptions, les risques de perte de données et les indisponibilités.

2 Nous opérons dans un environnement hautement sécurisé

Notre serveur est protégé par des mesures techniques garantissant un niveau de sécurité adapté au risque, parmi lesquelles :

- un accès à la console de configuration du serveur contrôlé par authentification à double facteur[3] (2FA) et strictement réservé à Lény Rolland (co-gérant) et Jacques Rolland (co-gérant) ;
- un accès au serveur lui-même par clé SSH[4] obligatoire, l'authentification par mot de passe étant désactivée, et strictement réservé à Lény Rolland et Jacques Rolland ;
- le chiffrement des données en transit (TLS/HTTPS) ;
- des sauvegardes régulières de l'intégralité de notre environnement de travail ;
- une séparation logique des environnements de développement, de test et de production, ainsi qu'un cloisonnement logique des environnements entre clients ;
- l'application régulière des mises à jour de sécurité et une gestion continue des vulnérabilités.

D'autre part, vous disposez d'un droit d'audit sur nos mesures de sécurité, que vous pouvez exercer vous-même ou par l'intermédiaire d'un tiers, dans les conditions prévues au DPA (préavis de quinze jours ouvrés, conditions raisonnables, hors auditeur concurrent, frais à la charge du Client sauf manquement constaté).

CGV art. 13.3, DPA P2 art. 4.3 et 6.2

POUR MIEUX COMPRENDRE

2 Un VPS (serveur privé virtuel) est un serveur disponible 24 heures sur 24 et 7 jours sur 7, installé dans un centre de données sécurisé situé au sein de l'Espace économique européen (EEE) dans notre cas, et que nous exploitons pour nos automatisations. Vos données y sont hébergées dans un environnement qui vous est dédié, isolé de ceux de nos autres clients et des autres utilisateurs de l'infrastructure.

3 L'authentification à double facteur exige deux preuves d'identité de nature différente pour se connecter : un mot de passe (ce que l'on sait) et un code temporaire généré sur un appareil personnel (ce que l'on possède). Ainsi, un mot de passe dérobé ne suffit pas pour outrepasser notre sécurité.

4 La clé SSH obligatoire, quant à elle, supprime totalement la connexion par mot de passe au serveur et la remplace par une paire de clés cryptographiques : une clé privée conservée par l'utilisateur, une clé publique installée sur le serveur. Les attaques par force brute ou par mot de passe deviné deviennent dès lors inopérantes.

02 La responsabilité de vos données

Avant de détailler les mesures de sécurité que nous mettons en place, nous souhaitons clarifier qui est responsable de quel type de donnée, au sens du RGPD.

TROIS RÔLES, AU SENS DU RGPD

Au sein d'une chaîne de traitement, le RGPD reconnaît trois rôles, selon la fonction réellement exercée : responsable du traitement, sous-traitant, sous-traitant ultérieur. De cette catégorisation découlent nos responsabilités sur les données.

Pour la grande majorité de nos prestations, vous restez **responsable du traitement**, nous intervenons comme **sous-traitant** et nos fournisseurs de logiciels comme **sous-traitants ultérieurs**.

Au sens du RGPD, le **responsable du traitement** est celui qui détermine les finalités d'un traitement ainsi que ses modalités. Pour les données de vos clients, vous conservez cette qualité en toute circonstance : c'est vous qui décidez des finalités poursuivies et des conditions dans lesquelles ces données sont traitées.

Il n'y a que pour les données vous concernant directement (votre numéro de téléphone professionnel, votre adresse e-mail professionnelle, votre SIRET, etc.) que nous sommes le **responsable du traitement**.

1 Traitements que Codesia opère en qualité de “responsable du traitement”

Concernant les données que nous traitons en qualité de responsable du traitement, vous disposez sur celles-ci des droits d'accès, de rectification, d'effacement, de limitation, de portabilité et d'opposition, que nous gérons au moyen d'une procédure formalisée. Les modalités d'exercice de ces droits sont précisées dans notre politique de confidentialité.

CGV art. 13.7 ; Politique de confidentialité art. 6 ; Procédure de gestion des demandes d'exercice des droits.

2 Traitements que Codesia opère en qualité de “sous-traitant”

L'article 28 du RGPD impose la conclusion d'un DPA[1] entre le responsable du traitement (vous) et le sous-traitant (Codesia), ainsi qu'un DPA entre le sous-traitant (Codesia) et chacun des sous-traitants ultérieurs (les logiciels tiers que nous utilisons).

Le DPA conclu entre le responsable du traitement et Codesia est systématiquement annexé au contrat de prestation. Il précise notamment :

- la nature et la finalité des traitements ;
- les catégories de données personnelles et de personnes concernées ;
- la durée des traitements ;
- les obligations respectives des Parties ;
- …

3 Traitements que les logiciels tiers opèrent en qualité de “sous-traitants ultérieurs”

Les DPA conclus entre Codesia (sous-traitant) et ses propres sous-traitants ultérieurs (les logiciels tiers que nous utilisons) sont également mis en place[2].

La liste des sous-traitants ultérieurs mobilisés pour chaque automatisation, leur rôle et la localisation des traitements figurent dans la fiche de l'automatisation annexée à votre contrat, que vous acceptez à la signature. Cette liste est confirmée dans la documentation de livraison. Avant tout ajout ou remplacement ultérieur, nous vous informons par écrit et vous disposez de quinze (15) jours pour émettre une objection motivée. Par exception, en cas de défaillance, de faille de sécurité ou de cessation d'activité d'un sous-traitant compromettant la continuité ou la sécurité de vos automatisations, nous procédons à son remplacement immédiat par un équivalent présentant des garanties équivalentes, vous en informons sans délai, et votre droit d'objection s'exerce alors a posteriori dans le même délai de quinze (15) jours.

CGV art. 13.3 ; DPA P2 art. 2 et 4.4 ; Documentation de livraison art. 6

POUR MIEUX COMPRENDRE

1 Le DPA (Data Processing Agreement) est un document qui définit ce que le prestataire (nous, ainsi que nos sous-traitants ultérieurs) est autorisé ou non à faire de vos données. Il formalise les obligations de chacune des parties et constitue l'instrument qui transforme une promesse commerciale de protection en engagement juridique opposable.

2 Pour certains fournisseurs, comme Anthropic ou Mistral, le DPA est incorporé par référence aux conditions de la plateforme : en acceptant ces conditions lors de la création du compte, nous acceptons automatiquement le DPA, sans démarche distincte. Pour d'autres, comme OpenAI, nous l'avons activé explicitement au moyen d'une procédure dédiée dans la console (saisie de l'entité et du signataire), à l'issue de laquelle le fournisseur nous a retourné le document contresigné.

03 La sécurisation de vos données

1 Vos données ne servent pas à entraîner les modèles d'IA

Notre architecture est conçue pour que vos données ne servent pas à entraîner les modèles d'IA. Nous opérons exclusivement via les API[1] professionnelles, dont les conditions excluent l'entraînement sur les données transmises ; nous activons les paramétrages d'exclusion disponibles et vérifions l'accord de traitement des données de chaque fournisseur. Cet engagement est contractualisé au titre d'une obligation de moyens : nous ne répondons pas du manquement d'un fournisseur tiers à ses propres engagements.

CGV art. 12.3 ; DPA P2 art. 4.7

2 Transmission et stockage de vos données à certains modèles d'IA

Nos automatisations font appel à des modèles d'IA externes, accessibles via leurs API professionnelles. Nous mettons en œuvre un ensemble de mesures destinées à limiter le risque au maximum.

- **Seules les données strictement nécessaires sont transmises** aux fournisseurs.
- La plupart de nos fournisseurs d'IA sont soumis au Cloud Act[2] américain (qui autorise les autorités américaines à exiger l'accès aux données détenues par un fournisseur américain) ; sur votre demande, vos automatisations peuvent être restreintes à des fournisseurs établis dans l'Union européenne, qui y échappent.
- Pour les fournisseurs américains, les données transmises via API ne sont, selon leurs politiques publiques, pas conservées au-delà de 30 jours (sauf situation exceptionnelle s'imposant au fournisseur, telle qu'une obligation légale ou une injonction judiciaire le contraignant à une conservation plus longue) ; via l'interface web classique, elles seraient conservées bien plus longtemps (18 mois par défaut chez Gemini, jusqu'à 5 ans chez Anthropic). Ces durées reflètent les politiques publiques des fournisseurs, consultées le 22/07/2026, et non un engagement contractuel de Codesia.
- Pour les sous-traitants établis hors UE, nous nous assurons soit de leur certification au Data Privacy Framework[3], soit de la mise en place de garanties appropriées au sens du RGPD (clauses contractuelles types notamment).

CGV, art. 3.4, 12.3 et 13.5 ; Contrat P3 art. 8.2 ; DPA P2 art. 4.5

3 Vos données restent strictement confidentielles

Nous sommes tenus à une obligation de confidentialité contractuelle, y compris sur les échanges précontractuels d'informations, notamment lors de l'appel découverte. Tout support (oral, écrit, électronique, visuel), qu'il soit désigné comme confidentiel ou non, y compris ce qui est observé sur site lors du diagnostic, est concerné. Cette obligation demeure pendant cinq (5) ans après la fin des relations commerciales et s'impose à nos sous-traitants et prestataires éventuels.

CGV articles 12.1, 12.2 et 12.5 ; DPA P2 articles 4.2 et 4.4

4 Usage et conservation de vos données par Codesia

L'usage de vos données est strictement limité à l'exécution du contrat, et leur accès est réservé à Lény Rolland (co-gérant) et Jacques Rolland (co-gérant). Vous demeurez propriétaire de l'intégralité de vos données, sur lesquelles nous ne détenons aucun droit en dehors de cette exécution.

- Nous n'exploitons jamais vos informations pour concevoir des solutions concurrentes, ni pour reproduire ou transposer vos processus métier chez d'autres clients.
- Si vous décidez de mettre fin au contrat, vous disposez de trente (30) jours pour choisir entre la restitution de vos données, dans un format structuré, couramment utilisé et lisible par machine, exécutée sous trente (30) jours, et leur suppression définitive attestée par écrit. À défaut de choix dans ce délai, nous supprimons vos données sous soixante (60) jours et l'attestons par écrit sur votre demande. Par ailleurs, nous désactivons tous les accès que nous avions à vos outils.

CGV art. 11.6, 12.2, 12.6, 18.2 et 18.3 ; DPA P2 art. 7 ; Documentation de transition art. 7 (rotation des secrets et révocation des accès) ; PSSI art. 4

5 Nous recensons rigoureusement toutes les activités de traitement

Nous tenons à jour un registre des activités de traitement, recensant l'ensemble des traitements de données personnelles que nous opérons, tant en qualité de responsable du traitement que de sous-traitant. Ce registre est disponible sur demande auprès des autorités compétentes.

CGV art. 13.6 ; DPA P2 art. 6.1

⚠ Nous demeurons attentifs à vos exigences en matière de souveraineté des données. Si vous souhaitez que nous n'ayons recours qu'à des modèles européens, de sorte qu'aucune donnée ne quitte jamais l'UE, nous nous y conformons.

POUR MIEUX COMPRENDRE

1 Une **API** (interface de programmation) est une porte d'entrée standardisée qui permet à deux logiciels de communiquer automatiquement entre eux. L'interface web que vous connaissez, le chat dans votre navigateur, est un produit conçu pour un humain : vous tapez, vous lisez, il y a un écran et un historique. L'API donne accès au même moteur d'IA, mais à destination de votre logiciel : la question est envoyée et la réponse reçue automatiquement, sans écran ni personne devant. Elle permet ainsi d'intégrer l'IA directement dans vos outils et de la faire travailler en volume sur vos processus.

2 Le **Cloud Act** (2018) est une loi américaine qui autorise les autorités américaines, lorsqu'elles estiment qu'une personne a commis une infraction pénale, à exiger d'une entreprise soumise au droit américain qu'elle leur livre les données qu'elle contrôle, quel que soit le pays où celles-ci sont physiquement stockées. Ces réquisitions demeurent toutefois, en pratique, très rares et ciblées, et le risque pesant sur vos données est quasiment nul.

3 Le **Data Privacy Framework** (DPF) est une décision d'adéquation de la Commission européenne (2023) qui autorise le transfert de données personnelles vers les entreprises américaines certifiées, reconnues comme offrant une protection équivalente à celle du RGPD. Ce cadre a été confirmé par le Tribunal de l'UE le 3 septembre 2025 (affaire Latombe). Un pourvoi reste pendant devant la CJUE, sans effet suspensif : le DPF demeure valide à ce jour. CODESIA suit ce dossier et adapte ses mécanismes de transfert si nécessaire.

04 Les mesures concernant l'IA spécifiquement

1 Classification du niveau de risque de nos automatisations

Nous classifions systématiquement nos automatisations selon les quatre niveaux décrits par l'AI Act (inacceptable, haut risque, limité et minimal). Cette classification, sa justification et les modalités d'usage recommandées vous sont communiquées dès le contrat de prestation, puis dans la documentation de livraison.

Nous nous interdisons de concevoir ou de déployer toute automatisation relevant des pratiques prohibées. L'usage des automatisations classées “à haut risque”, au sens de l'AI Act, fait quant à lui systématiquement l'objet d'une stipulation contractuelle.

Si un déploiement à haut risque est envisagé, il fait l'objet de conditions particulières dédiées qui organisent, entre vous et nous, l'ensemble des obligations propres à cette classification : à notre charge notamment la gestion des risques, la documentation technique et l'enregistrement du système dans la base de données de l'UE lorsqu'il est requis ; à votre charge notamment la supervision humaine effective, la conservation des journaux pendant six (6) mois minimum, l'usage conforme aux instructions des fournisseurs et l'information des personnes concernées, avec notre assistance.

CGV art. 14.2 et 14.6 ; Contrat de prestation P2 art. 3.1 et 8.1 ; PV de réception art. 4 ; Documentation de livraison art. 3

2 Mécanismes de supervision humaine (“human in the loop”)

Nous intégrons dès la conception des mécanismes de contrôle et de supervision proportionnés au niveau de risque. La liste des cas où une supervision humaine est requise vous est communiquée dans la documentation de livraison.

CGV art. 8.5 et 14.5 ; Contrat P2 art. 8.3 ; Documentation de livraison art. 4

3 Transparence quant à l'utilisation de systèmes d'IA

Nous intégrons dès la conception les mécanismes nécessaires pour signaler l'interaction avec une IA ou le caractère généré par IA d'un contenu.

Nous mettons en œuvre les mécanismes nécessaires pour que les utilisateurs amenés à interagir avec une IA en soient informés au plus tard lors de la première interaction ; la mise en œuvre opérationnelle vous incombe toutefois.

L'information des personnes appelées à utiliser une automatisation classée “à haut risque” incombe au Client déployeur, avec notre assistance.

CGV art. 14.3 et 14.6 ; AI Act art. 50(1) et 26(7) ; Documentation de livraison art. 5

05 Pour conclure

1 Veille réglementaire continue

Nous menons une veille réglementaire continue[1] sur l'évolution des cadres légaux applicables à notre activité, afin d'anticiper les obligations à venir et d'adapter nos prestations en conséquence. Le présent document, mais aussi et surtout l'ensemble des documents juridiquement opposables qui en constituent les sources, sont régulièrement mis à jour pour refléter les dernières exigences applicables.

De même, toutes les mesures de sécurité présentées ci-dessus sont réévaluées périodiquement, en fonction de l'état de l'art et de l'évolution des risques.

DOCUMENTATION — VERSION 1.5
26/10/2026

2 Engagement environnemental et social

Notre VPS est hébergé dans un centre de données situé au sein de l'Espace économique européen (EEE), dont la consommation électrique est couverte à 100 % par de l'électricité renouvelable. L'infrastructure est certifiée ISO 14001 et ISO 50001, les deux normes internationales de management environnemental et énergétique. Notre prestataire met également en œuvre une compensation carbone sur ses centres de données.

L'IA doit être à votre service, jamais l'inverse. C'est un outil destiné à supprimer les tâches étrangères à votre expertise et dépourvues de valeur formatrice, au profit d'un temps précieux pour réfléchir et innover, pour élaborer de nouvelles méthodes de travail, pour créer du lien avec vos collègues ; du temps pour vous développer et retrouver du sens.

Pour garantir que l'IA s'intègre harmonieusement dans votre environnement, nous prenons très à cœur les recommandations dites d'AI Literacy de l'AI Act. Nous intégrons un transfert systématique de compétences lors de la remise des déploiements, ainsi qu'un suivi dans la durée, afin de répondre à vos questions et de garantir que vous conserviez une pleine compréhension et maîtrise de ces outils.

CGV art. 3.3, 8.4, 14.4 et 9.2 ; Contrat P2 art. 7 ; PV de réception P2 art. 6 ; Contrat P3 art. 6. Conformité AI Act : article 4.

POUR MIEUX COMPRENDRE

1 Dernière évolution majeure : le Digital Omnibus, approuvé par le Parlement européen le 16 juin 2026, adopté par le Conseil le 29 juin, publication au Journal officiel de l'UE attendue avant le 2 août 2026. Il reporte les obligations des systèmes à haut risque de l'annexe III (recrutement, biométrie) du 2 août 2026 au 2 décembre 2027 ; avant publication, l'échéance du 2 août 2026 reste la référence légale. Les obligations de transparence de l'article 50 (mention IA, marquage des contenus générés) ne sont pas reportées et s'appliquent au 2 août 2026 : nos déploiements les intègrent. Nos usages, automatisations métier hors domaines sensibles, ne relèvent pas du haut risque : aucune démarche nouvelle pour vous. Nos conditions générales renvoient aux dispositions applicables à la date de livraison. Nous suivons ces évolutions en continu ; votre dispositif est d'ores et déjà aligné.